IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

Edward Polhill and Steven Vash, individually and on behalf of all others similarly situated, Plaintiffs, vs. T-Mobile US, Inc., Defendant.	CASE NO. **COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiffs Edward Polhill ("Plaintiff Polhill") and Steven Vash ("Plaintiff Vash" and collectively with Plaintiff Polhill, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant T-Mobile US, Inc. ("T-Mobile" or "Defendant") based on their personal knowledge and the investigation of counsel and allege as follows:

INTRODUCTION

1. This is a class action brought by Plaintiffs on behalf of themselves and the other similarly situated persons whose personal information was acquired and/or accessed by unauthorized persons in the data breach that T-Mobile describes through its filing with the Securities and Exchange Commission (the "SEC") dated January

19, 2023 (the "2023 Data Breach").

2. Upon information and belief, Plaintiffs and the proposed class members first learned of the 2023 Data Breach through news outlets reporting the breach on January 20, 2023.

3. The 2023 Data Breach has been estimated to impact 37 million present and former customers of T-Mobile. However, as T-Mobile is one of the largest technology companies in the United States, the 2023 Data Breach could have involved and could affect hundreds of millions of current and former T-Mobile customers.

4. The 2023 Data Breach affected individuals whose information was stored on T-Mobile's servers in multiple states.

5. T-Mobile provides wireless voice, messaging, and data services in the United States, including Puerto Rico and the U.S. Virgin Islands under the T-Mobile and Metro by T-Mobile brands. The company operates the second largest wireless network in the U.S. market, with over 110 million customers and annual revenues of more than $80 billion.

6. Plaintiffs and other members of the proposed class were required, as current and former customers of T-Mobile, to provide T-Mobile with sensitive personal information to apply for and/or receive wireless voice, messaging, and data services. T-Mobile assured Plaintiffs and other members of the proposed class that

their personal information would be kept safe from unauthorized access. The T-Mobile Privacy Policy touts the following: "You, as consumers, trust T-Mobile to connect you to the world every day, and we're working hard to earn a place in your heart. A big part of that is maintaining your privacy…. We use administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control."[1]

7. T-Mobile betrayed the trust of Plaintiffs and other members of the proposed class by failing to properly safeguard and protect their sensitive personal information, enabling cybercriminals to acquire and/or access it.

8. Upon information and belief, the data subject to the 2023 Data Breach was sensitive personal information that was unencrypted and unredacted and compromised by Defendant's failure to take proper safeguards of the information.

9. Defendant's failure to secure its users' sensitive personal information is particularly egregious given the known dangers of security hacks and data breaches generally, and T-Mobile's own numerous, significant, and serious prior data breaches.

10. Plaintiffs brings this class action against T-Mobile for its failure to properly secure and safeguard the sensitive and personally identifiable contact and

[1] *Privacy Notice*, T-Mobile: Privacy Center, Dec. 22, 2022, https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice.

demographic information of Plaintiffs and other members of the proposed class stored within T-Mobile's information network, including, but not limited to, first and/or last name, billing address, email, phone number, date of birth, T-Mobile account number and information such as the number of lines on account and account plan features (these types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII").[2]

11. T-Mobile disregarded the rights of Plaintiffs and the other members of the proposed class by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and other members of the proposed class was safeguarded.

12. Specifically, T-Mobile ignored the rights of Plaintiffs and other members of the proposed class by, inter alia, intentionally, willfully, recklessly or negligently failing to: (1) ensure the security and confidentiality of consumer records and PII; (2) protect against anticipated threats or hazards to the security or integrity of consumer records and PII; (3) protect against unauthorized access to or use of consumer records or PII that could result in substantial harm or inconvenience

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands.

to any current or prospective customer; (4) implement or maintain policies and procedures that adequately secured consumers' records and PII; (5) sufficiently monitor, audit and update its cybersecurity procedures and patch maintenance; and (6) timely detect the 2023 Data Breach, mitigate harm, and notify consumers of the 2023 Data Breach. As a result, the PII of Plaintiffs and other members of the proposed class was compromised through disclosure to and access by one or more unknown and unauthorized third parties.

13. Plaintiffs and other members of the proposed class have suffered injury because of T-Mobile's conduct. These injuries include: (a) invasion of privacy; (b) actual identity theft; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2023 Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiffs' and the prospective class members' PII in their continued possession; (g) future costs in terms of time, effort, and money that will be expended as a result of the 2023 Data

Breach for the remainder of the lives of Plaintiffs and other members of the proposed class; and (h) the diminished value of Plaintiffs' and the prospective class members' PII; (i) the diminished value of T-Mobile's services Plaintiffs and other members of the proposed class paid for and received; and/or (j) the actual and attempted sale of Plaintiffs' and the prospective class members' PII on the dark web.

14. In addition to remedying the harms suffered because of the 2023 Data Breach, Plaintiffs and the more than 37 million customers similarly situated also have a significant interest in preventing additional data breaches because their PII remains in T-Mobile's possession without adequate protection.

15. Representative Plaintiffs bring this action on behalf of all persons whose PII was compromised because of T-Mobile's failure to: (i) adequately protect the PII of Plaintiffs and other members of the proposed class; (ii) warn Plaintiffs and other members of the proposed class of these inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. T-Mobile's conduct amounts to negligence and violates federal and state statutes.

16. Plaintiffs, for themselves and for others similarly situated current and former customers of T-Mobile impacted by the 2023 Data Breach, seek actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses. Plaintiffs also seek declaratory and injunctive relief, including

significant improvements to T-Mobile's data security systems and protocols (which have been the subject of multiple recent data breaches), future annual audits, T-Mobile-funded long-term credit monitoring services, and any other remedies the Court deems necessary and proper.

THE PARTIES

17. Plaintiff Polhill is a citizen and resident of the State of Michigan and was a Michigan resident during the period when the 2023 Data Breach occurred.

18. Plaintiff Polhill is and has been a customer of, and received wireless voice, messaging, and data services from, T-Mobile. The reports regarding the breadth and severity of the 2023 Data Breach and T-Mobile's disclosures concerning the number and class of consumers affected indicate, upon information and belief, that Plaintiff Polhill and his data have been impacted.

19. Plaintiff Vash is a citizen and resident of the State of Georgia and was a Georgia resident during the period when the 2023 Data Breach occurred.

20. Plaintiff Vash is and has been a customer of, and received wireless voice, messaging, and data services from, T-Mobile. The reports regarding the breadth and severity of the 2023 Data Breach and T-Mobile's disclosures concerning the number and class of consumers affected indicate, upon information and belief, that Plaintiff Vash and his data have been impacted.

21. To receive wireless voice, messaging, and data services from T-Mobile,

Plaintiffs were required to provide T-Mobile with sensitive PII. Plaintiffs' PII was within the possession and control of T-Mobile at the time of the 2023 Data Breach.

22. Plaintiffs brings this action on behalf of themselves, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

23. Defendant T-Mobile US, Inc. is a Delaware corporation with its principal place of business located at 12920 SE 38th Street, Bellevue, Washington 98006. T-Mobile has a corporate office located at 1 Ravinia Dr. NE, Atlanta, Georgia 30346.

24. T-Mobile provides wireless voice, messaging, and data services in the United States, including Puerto Rico, and the U.S. Virgin Islands, under the T-Mobile and Metro by T-Mobile brands. The company operates the second largest wireless network in the U.S. market with over 110 million customers.

25. T-Mobile has access to enormous resources. In 2021, T-Mobile reported total revenues of more than $80 billion and net income of more than $3 billion. In that same fiscal year, T-Mobile reported total assets of more than $206 billion.

JURISDICTION AND VENUE

26. This Court has diversity jurisdiction over this action pursuant to 28

U.S.C. §1332 because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and upon information and belief, at least one other member of the proposed class is a citizen of a state different from Defendant.

27. This Court has personal jurisdiction over Defendant because Defendant has a corporate office in the State of Georgia, routinely conducts business in Georgia, has sufficient minimum contacts in Georgia, and has intentionally availed itself of this jurisdiction by marketing and selling products and services in Georgia.

28. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant has a corporate office located in the District, Defendant conducts a substantial amount of its business in this District, and the events that give rise to Plaintiffs' claims occurred in part in this District.

FACTUAL ALLEGATIONS

The Breach

29. On January 20, 2023, the 2023 Data Breach was first reported by various news outlets, including through the USA Today article entitled, *In **latest** T-Mobile hack, 37 million customers have personal data stolen, company says* (emphasis added).[3] According to the aforementioned report, "a 'bad actor' stole

[3] Wyatte Grantham-Philips, *In latest T-Mobile hack, 37 million customers have personal data stolen, company says*, USA Today, Jan. 20,

personal information from approximately 37 million T-Mobile customers in a November [2022] data breach."[4]

30. In its 8-K filing with the SEC dated January 19, 2023, T-Mobile stated:

> On ***January 5, 2023***, T-Mobile US, Inc. (the "Company," "we," or "our") identified that a bad actor was obtaining data through a single Application Programming Interface ("API") without authorization…. ***We currently believe that the bad actor first retrieved data through the impacted API starting on or around November 25, 2022***. We are continuing to diligently investigate the unauthorized activity. In addition, we have notified certain federal agencies about the incident, and we are concurrently working with law enforcement. Additionally, we have begun notifying customers whose information may have been obtained by the bad actor in accordance with applicable state and federal requirements.

(emphasis added).

31. Thus, T-Mobile did not discover the 2023 Data Breach until ***forty*** days after it was initiated and its investigation of the breach remains ongoing.

Plaintiffs' Dealings with T-Mobile

32. Plaintiffs are and have been T-Mobile customers since before the 2023 Data Breach and provided personally identifiable information to T-Mobile in order to maintain postpay mobile services from T-Mobile.

T-Mobile Understood the Value of PII

33. In connection with providing services to Plaintiffs, members of the proposed class and its other millions of customers, T-Mobile collects and maintains

---

2023, https://www.usatoday.com/story/tech/2023/01/20/tmobile-data-hack-37-million-customers/11088603002/.

[4] *Id.*

massive amounts of sensitive PII, including information that users cannot simply change if there is a breach, including, but not limited to, their names, demographic information, and birth dates.

34. Present and former customers like Plaintiffs and the other members of the proposed class entrust Defendant with their PII with the understanding that, as T-Mobile has promised, T-Mobile would keep their PII safe and secure.

35. T-Mobile understands the importance of protecting PII. Through its Privacy Policy, T-Mobile's states as follows: "We use administrative, technical, contractual, and physical safeguard designed to protect your data while it is under our control."

36. Notwithstanding these promises, it appears at least one hacker was able to breach T-Mobile's servers and acquire the sensitive PII of more than 37 million current and former customers of T-Mobile. There is, therefore, little question that T-Mobile did not to live up to its promises regarding data protection.

37. There have been several significant data breaches targeting consumers and their PII at other companies during the last several years, including at Marriott (500 million in 2018); Facebook (540 million in 2019); Capital One (106 million in 2019); and Estee Lauder (440 million in 2020).

38. As T-Mobile has also been the subject of multiple data breaches in recent years, it should have been on high alert, particularly with regard to

cybersecurity maintenance.

39. In the past five years, T-Mobile has suffered at least ***seven*** additional large breaches:

> In August 2018, the company said that 3% of its customer data was leaked. An attacker was exfiltrating personal data such as customer names, billing ZIP codes, phone numbers, email addresses, account numbers, and account types (prepaid or postpaid).
>
> In 2019, November, the company disclosed that the account information of an undisclosed number of prepaid customers was accessed by an unauthorized third party. In March 2020, T-Mobile announced a data breach caused by an email vendor being hacked that exposed the personal and financial information of some of its customers. In the same year in December, the company suffered another breach that exposed customers' proprietary network information (CPNI), including phone numbers and call records.
>
> T-Mobile again disclosed a data breach after an unknown number of customers were affected by SIM swap attacks in February 2021. The telecommunications giant had warned that information including names, dates of birth, US Social Security numbers (SSNs), and driver's license/ID of some 77 million individuals comprising current, former, or prospective customers had been exposed via a data breach in August 2021.
>
> However, its ordeal didn't end with this. In another incident in April 2022, Lapsus$, a hacker group, was able to gain access to the company's internal tools, which gave them the chance to carry out SIM swaps.[5]

40. In 2022, pursuant to the settlement of one of its many data hacks, T-

[5] Apurva Venkat, *T-Mobile suffers 8th data breach in less than 5 years*, CSO Online, Jan. 20, 2023, https://www.csoonline.com/article/3686053/t-mobile-suffers-8th-data-breach-in-less-than-5-years.html.

Mobile agreed to invest $150 million to upgrade its cybersecurity. However, as the 2023 Data Breach shows, notwithstanding that promised investment, serious security lapses persist.[6]

41. Upon information and belief, T-Mobile did not use reasonable security procedures and practices commensurate with the type of sensitive customer information it was maintaining. Consequently, Defendant caused the PII of Plaintiffs and the member of the proposed class to be vulnerable to hackers, thieves and other bad actors.

42. Upon information and belief, the cyberattack that resulted in the 2023 Data Breach was specifically designed to gain access to T-Mobile customers' private and confidential data, including the PII of Plaintiffs and other members of the proposed class.

43. As a multi-billion-dollar company, T-Mobile had the resources necessary to invest in security measures to prevent the 2023 Data Breach, but Defendant failed to adequately invest in that security, despite its promises and obligations to protect its users' PII.

44. T-Mobile could have prevented this latest data breach by taking, developing and/or implementing policies and procedures, including computer data security programs, that would have provided the level of protection appropriate and

[6] *Id.*

reasonably necessary for a company of T-Mobile's size and sophistication, which also held substantial amounts of PII for tens of millions of people, as well as given Defendant's history of known data security issues.

45. Consumers have many choices for wireless voice, messaging, and data services, and Plaintiffs and the members of the prospective class would not have chosen to provide their PII to T-Mobile had they known that the information would be at a heightened risk of compromise due to T-Mobile's persistently lax data security.

Plaintiffs and Prospective Class Members Have Suffered Harm

46. As a result of the 2023 Data Breach, Plaintiffs and the prospective class members were deprived of the value in and security of their PII and now face an increased risk of theft, identity theft, fraud, and abuse, and the constant fear, anxiety, and hardship that comes with it. Further, those impacted by T-Mobile's failure to protect Plaintiffs' and the prospective class members' PII will be at risk for identity theft and fraud for years to come.

47. As a result of T-Mobile's unfair, inadequate, and unreasonable data security, at least one cyber-criminal and unknown others now possess the PII of Plaintiffs and the prospective class members.

48. It is well known that stolen PII is a valuable commodity for hackers.[7] As a result, PII is a frequent target of their attacks.[8] A "cyber black-market" exists in which criminals openly post sensitive personal information for sale.

49. The sensitive personal information that T-Mobile failed to adequately protect is "as good as gold" to identity thieves. Identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name and incur charges on existing accounts.[9] Further, criminals can file false federal and state tax returns in victim's names, preventing or at least delaying victims' receipt of their legitimate tax refunds and potentially making victims targets of IRS and state tax investigations.[10] Victims' credit profiles can be destroyed, and they can lose the ability to legitimately borrow money, obtain credit, or even open bank accounts.

---

[7] Patricia Ruffio, Dark Web Price Index 2022, Privacy Affairs, Sept. 19, 2022, https://www.privacyaffairs.com/dark-web-price-index-2022/ (setting forth 2021-2022 dark web average prices for PII and other stolen information).

[8] Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS News Hour, May 14, 2021, https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it ("Though data breaches can be a national security threat, 86% are about money…. Stolen data often ends up being sold online on the dark web…. Buyers use stolen data in several ways. Credit card numbers and security codes can be used to create clone cards for making fraudulent transactions. Social Security numbers, home addresses, full names, dates of birth and other personally identifiable information can be used in identity theft. For example, the buyer can apply for loans or credit cards under the victim's name and file fraudulent tax returns.").

[9] *Id.*

[10] Nat Sillin, What To Do If Someone Files A False Tax Return in Your Name, National Foundation for Credit Counseling, August 21, 2015, https://www.nfcc.org/blog/what-to-do-if-someone-files-a-false-tax-return-in-your-name/.

50. In addition to stolen personal information being "fuel for identity theft… [w]ith stolen personal information criminals can target victims with phishing attacks," luring victims into unknowingly providing sensitive information to bad actors.[11]

51. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, social security numbers, and other PII directly on various Internet websites and on the dark web, making the information publicly available and available to criminals. And, unlike a stolen credit card number, which can be changed or the associated account closed, certain of the PII stolen in the 2023 Data Breach has even greater long-term value for thieves, as it cannot be altered in the same way.

52. At the very least, victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, get student loans, or buy or rent furniture or a new TV, let alone complete a major purchase such as a new car or home, without taking the time to request that

[11] *Why Do Hackers Want Your Personal Information?*, F-Secure, https://www.f-secure.com/en/home/articles/why-do-hackers-want-your-personal-information.

the freeze be suspended, waiting the days it can take for that to occur, and then reinstating the freeze. Further, there are four major reporting agencies, so consumers may need to take these steps with all of them because they will not know which bureau a creditor may consult. Also, in many states, and in many circumstances, such freezes cost the consumer money.

53. Moreover, credit monitoring services do little to prevent wholesale identity theft. Further, experts warn that batches of stolen information may not be immediately dumped on the black market, thus leaving victims vulnerable to attack for an indefinite period of time. "[O]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed.... They often wait until consumers are less likely to be on the lookout for fraudulent activities."[12] "It would be wise for a criminal to just hold on to [PII] for a few years and wait until people are less vigilant."[13]

54. A cybercriminal, especially one with millions of records, can hold on to stolen information for years until the news of the theft has subsided, then steal a victim's identity, credit, and bank accounts, or engage in other bad acts to exploit the theft of PII, resulting in a victim suffering thousands of dollars in losses and lost

[12] AnnaMaria Andriotis, *Into the Breach: Identity-Theft Protection*, The Wall Street Journal, Jan. 24, 2014, https://www.wsj.com/articles/into-the-breach-identitytheft-protection-1390607608?tesla=y.
[13] David Lazarus, *So what does a corporation owe you after a data breach?*, The Los Angeles Times, May 10, 2016, https://www.latimes.com/business/lazarus/la-fi-lazarus-security-breaches-20160510-snap-story.html.

time and productivity. Thus, Plaintiffs and members of the proposed class must take additional steps to protect their identities as well as bear the burden and expense of identity and credit monitoring, and heightened vigilance for years to come.

55. Despite the FTC's warnings about data theft and the many public announcements of data breaches and data security compromises, as well as its own multiple well publicized data breaches, T-Mobile failed to take the appropriate steps to protect the PII of Plaintiffs and members of the proposed class.

56. Unquestionably, T-Mobile had ample resources to invest, and in fact had been mandated to invest, in the needed security measures. Moreover, there is much guidance setting forth the accepted security measures in Defendant's industry.

57. The National Institute of Standards and Technology (the "NIST") regularly provides guidance and advice on the various cybersecurity practices organizations should employ to maintain the security of consumer PII stored in their servers in the form of a cybersecurity framework consisting of five major functions of cybersecurity organizations must engage in to maintain sufficient security standards.

58. Among more detailed standards, the NIST Cybersecurity Framework provides the following guidance:

a. Identify the organization's asset management, business environment, governance, risk assessment, risk management strategy, and supply chain risk management;

b. Protect through identity management and access control, personnel awareness and training, implementing data security, implementing information protection processes and procedures, maintenance, and protective technology;

c. Detect anomalies and events through continuous security monitoring to identify cybersecurity events and verify the effectiveness of protective measures, and through detection processes that are maintained and tested to ensure awareness of anomalous events.

d. Respond with a response plan, communication with internal and external stakeholders, analysis to ensure effective response and support recovery activities, mitigation activities to prevent expansion of the event and effects, and improvements to the response plan for future cybersecurity events;

e. Recover by executing recovery plans and procedures to ensure restoration of affected systems or assets, improving upon recovery planning and processes by incorporating lessons learned, and communicating recovery activities to internal and external stakeholders as well as executive and management teams.[14]

59. The FTC provides an overarching data security plan built on similar principles to the NIST guidance detailed above. According to the FTC, "[a] sound data security plan is built on 5 key principles:"

a. Take Stock. Know what personal information is on your computers.

b. Scale Down. Keep only what is needed for business.

c. Lock It. Protect the information that is kept.

d. Pitch it. Properly dispose of information that is no longer needed.

[14] Stephen Quinn et al., *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight, NIST IR 8286C*, National Institute of Standards and Technology: Computer Security Resource Center, Sept. 2022, https://csrc.nist.gov/publications/detail/nistir/8286c/final.

e. Plan Ahead. Create a plan to respond to security incidents.[15]

60. The FTC provides more specific guidance regarding security including the following directives:

a. Identify the computers or servers where sensitive personal information is stored;

b. Assess the vulnerability of computers and servers to commonly known or reasonably foreseeable attacks;

c. Implement policies to update and correct and security problems;

d. Only store consumer data that is essential for conducting business purposes;

e. Encrypt sensitive information sent to third parties over public networks;

f. Encrypt sensitive information stored on the computer network, laptops, or portable storage devices used by employees;

g. Regularly run up-to-date anti-malware programs on individual computers and on servers on the network;

h. Use Transport Layer Security (TLS) encryption or another secure connection to protects when receiving or transmitting personal identifying information;

i. Control access to sensitive information by requiring "strong" passwords;

j. Requiring and implementing multi-factor authentication;

k. Caution against transmitting sensitive personally identifying data via email;

l. Implement a firewall for protection from internet hackers. Further, determine whether a "border" firewall is needed where the network connects to the internet;

m. Encrypt information sent over wireless networks;

n. Only use wireless routers with Wi-Fi Protected Access 2 (WPA2) capability and devices that support WPA2;

[15] *Protecting Personal Information: A Guide for Business,* Federal Trade Commission: Business Guidance Resources, Oct. 2016, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business#takestock.

o. Maintain central logs of security-related information to monitor activity and respond to possible attacks;

p. Utilize intrusion detection systems;

q. Monitor incoming traffic for suspicious behavior and/or large amounts of transmitted data;

r. Monitor outgoing traffic for suspicious behavior and/or large amounts of transmitted data;

s. Train employees to recognize security threats;

t. Before outsourcing business functions investigate the third-party company's data security to ensure reasonable security measures;

u. Limit employee and vendor access to sensitive data; and

v. Utilize industry-tested methods for security.[16]

61. Upon information and belief, T-Mobile failed to comply with one or more of these standards.

62. To date, Defendant has failed to adequately protect Plaintiffs and the prospective class members or to compensate them for their injuries sustained in the 2023 Data Breach.

63. As a result, due to the actual and imminent risk of identity theft, Plaintiffs and the prospective class members must, in Defendant's words, "remain vigilant" and monitor their financial accounts for the foreseeable future, and possibly the rest of their lives, to mitigate the risk of identity theft or other harm.[17]

64. Plaintiffs and the prospective class members have spent, and must

[16] *Id.*
[17] *Online Safety and cybersecurity*, T-Mobile: Privacy Center, https://www.t-mobile.com/privacy-center/education/online-safety-cybersecurity.

continue to spend additional time in the future, on a variety of prudent actions, such as placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and/or filing police reports.

65. Plaintiffs' and the prospective class members' mitigation efforts are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches in which it notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[18]

66. Plaintiffs' and the prospective class members' mitigation efforts are also consistent with the steps recommended to data breach victims by the FTC, which include: contacting one of the credit bureaus to place a fraud alert (including a seven year alert if identity theft occurs); constant and prudent review of their credit reports; contacting companies to remove fraudulent charges from their accounts; placing freezes on their credit; and correcting credit reports.[19]

67. Furthermore, Defendant's poor data security deprived Plaintiffs and the prospective class members of the benefit of their bargain. When agreeing to pay

[18] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO-07-737, U.S. Government Accountability Office, Jul. 7, 2007. https://www.gao.gov/assets/a262904.html.

[19] IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/#/Info-Lost-or-Stolen.

Defendant services, Plaintiffs and the prospective class members as Defendant's customers understood and expected that they were paying for services and data security, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and the prospective class members received services of lesser value than they reasonably expected and paid for.

68. As a result of Defendant's ineffective and inadequate data security and retention measures, the 2023 Data Breach, and the imminent risk of identity theft, Plaintiffs and the prospective class members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial costs incurred in mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and productivity incurred in mitigating the materialized risk and imminent threat and risk of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of the benefit of their bargain; (h) deprivation of the value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and the prospective class members' personal sensitive information.

69. Plaintiffs and the prospective class members provided their personal information to Defendant and/or its affiliates in conjunction with the product and

services Plaintiffs obtained.

70. As part of their involvement with Defendant, Plaintiffs entrusted their PII, and other confidential and sensitive information such as name, address, phone number, financial account information, and other personally identifiable information to Defendant and its affiliates with the reasonable expectation and understanding that they would at a minimum take standard industry precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify her of any data security incidents related thereto. Plaintiffs would not have permitted their PII to be given to Defendant had they known they would not take reasonable steps to safeguard their PII.

71. As a result of the 2023 Data Breach, Plaintiffs have or will make reasonable efforts to mitigate the impact of the 2023 Data Breach, including but not limited to, researching the 2023 Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

72. Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) damage to and the diminution in value of their PII, a form of property Defendant obtained from Plaintiffs; (b) violation of their privacy rights; (c) theft of their; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

CLASS ACTION ALLEGATIONS

73. Representative Plaintiffs brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following class (collectively, the "Class"):

> All persons residing in the United States whose personal information was acquired or accessed by unauthorized individuals as a result of the breach of T-Mobile US, Inc.'s information system(s) that was reported in its January 19, 2023 8-K filing.

74. The following individuals and entities are excluded from the proposed Class: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

75. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

76. **Numerosity**: The proposed Class is believed to be so numerous that joinder of all members is impracticable. Upon information and belief, the total number of Class members is in the millions of individuals. Membership in the classes will be determined by analysis of Defendant's records.

77. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class ("Class Members") were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class Member because Plaintiffs and each Class Member had their PII compromised in the same way by the same conduct of Defendant.

78. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

79. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized

litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

80. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant had a duty not to disclose the Plaintiffs' and Class members' PII to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard Plaintiffs' and Class members' PII;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether Defendant breached this duty;

e. Whether Defendant's systems, networks, and data security practices used to protect Plaintiffs' and Class Members' PII

violated the FTC Act, and/or Defendant's other duties discussed herein;

f. Whether Defendant knew or should have known that their computer and network security systems were vulnerable to a data breach;

g. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the 2023 Data Breach;

h. Whether Defendant breached contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

i. When Defendant actually learned of the 2023 Data Breach;

j. Whether Defendant failed to adequately respond to the 2023 Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

k. Whether Defendant fully and adequately addressed and fixed its systems' vulnerabilities which permitted the 2023 Data Breach to occur;

l. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiffs' and Class Members'

PII;

m. Whether Defendant continues to breach duties to Plaintiffs and the Class;

n. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

o. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

p. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members and the public;

q. Whether Defendant's actions alleged herein constitute gross negligence; and

r. Whether Plaintiffs and Class Members are entitled to punitive damages.

81. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's policies challenged herein apply

to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to the Plaintiffs.

82. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

CLAIMS FOR RELIEF

Count I
Negligence

83. Plaintiffs incorporates by reference the allegations in paragraphs 1 through 82 above as though fully set forth herein.

84. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard the PII of Plaintiffs and Class Members and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiffs and Class members in its computer systems and on its networks.

85. In order to use Defendant's goods and services, Plaintiffs and Class Members were obligated to provide Defendant with their PII, including, their names, addresses, dates of birth, personal addresses and other sensitive personal

information, depending upon the product or service.

86. Among Defendant's duties, Defendant was expected to:

a. Exercise reasonable care in obtaining, retaining, securing, and protecting PII in its possession;

b. Protect Plaintiffs' and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;

c. Exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication, including patch maintenance;

d. Adequately monitor, audit, and update the security of its networks and systems including patch maintenance;

e. Implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

f. Recognize in a timely manner that Plaintiffs' and other Class Members' PII had been compromised;

g. Promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected

their PII; and

h. Timely detect and mitigate the 2023 Data Breach.

87. Defendant knew that the PII of Plaintiffs and Class Members was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

88. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

89. Defendant knew, or should have known, that cyber criminals routinely target large corporations through cyberattacks to steal sensitive personal information.

90. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

91. Because Defendant knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained thereon.

92. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' PII and

promptly notify them about the 2023 Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiffs and Class Members.

93. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII its stored on them from attack.

94. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and Class Members.

95. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class Members.

96. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. Failing to exercise reasonable care in obtaining, retaining, securing, and protecting PII in its possession;

b. Failing to protect Plaintiffs' and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;

c. Failing to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures, and practices to ensure that Plaintiffs' and Class Members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication;

d. Failing to adequately train its employees to not store PII longer than absolutely necessary;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class Members' PII;

f. Failing to implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers;

g. Failing to adhere to the applicable industry standards for cybersecurity and exercise reasonable care, thus leaving Plaintiffs' and the Class Members' PII vulnerable to theft;

h. Failing to heed industry warnings and alerts to provide sufficient safeguards to protect Plaintiffs' and Class Members' PII in the face of known risks of hackers and theft; and

i. Failing to promptly notify Plaintiffs and Class Members of any

data breach, security incident, or intrusion that affected or may have affected their PII.

97. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

98. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access by failing to notify Plaintiffs and Class Members immediately after learning of the 2023 Data Breach and then by failing to provide Plaintiffs and Class Members sufficient information regarding the breach.

99. Further, through its failure to provide timely and clear notification of the 2023 Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

100. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and Class Members. Plaintiffs' and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

101. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred because of Defendant's failure to observe these duties, including the loss of privacy, significant risk of identity theft, and Plaintiffs' and Class Members' overpayment for goods and services, are the types of harm that these statutes and their regulations were intended to prevent.

102. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiffs and Class Members to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

103. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

104. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

105. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

106. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' PII, and by failing to provide prompt notice without reasonable delay.

107. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

108. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

109. The harm that occurred because of the 2023 Data Breach is the type of harm the FTC Act was intended to guard against.

110. Defendant breached its duties to Plaintiffs and Class Members under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

111. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to: (a) invasion of privacy; (b) actual identity theft; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and

attempting to mitigate the actual and future consequences of the 2023 Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII in their continued possession; (g) future costs in terms of time, effort, and money that will be expended as a result of the 2023 Data Breach for the remainder of the lives of Plaintiffs and other Class Members; and (h) the diminished value of Plaintiffs' and Class Members' PII; (i) the diminished value of T-Mobile's services Plaintiffs and other Class Members paid for and received; and/or (j) the actual and attempted sale of Plaintiffs' and Class Members' PII on the dark web.

112. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

Count II
Invasion of Privacy

113. Plaintiffs incorporates by reference the allegations in paragraphs 1 through 82 above as though fully set forth herein.

114. Plaintiffs and Class Members had a legitimate and reasonable

expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

115. Defendant owed a duty to Plaintiffs and Class Members to keep their PII confidential.

116. Defendant allowed unauthorized and unknown third parties access to and acquire the PII of Plaintiffs and Class Members because it failed to protect and implement adequate security measures for the PII.

117. The unauthorized access to, acquisition of, and/or viewing of the PII of Plaintiffs and Class Members by unauthorized third parties is highly offensive to a reasonable person.

118. Defendant's willful and reckless conduct which enabled the theft and disclosure of Plaintiffs' and Class Members' sensitive and confidential personal information is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

119. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of obtaining services from Defendant, but privately and with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their

belief that their disclosure of private facts in the form of PII would be kept private and would not be disclosed without their authorization and the disclosure of their PII through the 2023 Data Breach was wholly without their consent, and in violation of state and federal law.

120. The 2023 Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

121. Defendant acted with a knowing state of mind when it permitted the 2023 Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

122. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

123. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class members to suffer damages.

124. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be

accessed, acquired, and viewed by unauthorized persons for years to come.

125. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs or Class members.

Count III
Unjust Enrichment

126. Plaintiffs incorporates by reference the allegations in paragraphs 1 through 82 above as though fully set forth herein.

127. Plaintiffs and Class Members paid for Defendant's products and services.

128. As Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiffs and Class Members.

129. The funds that Plaintiffs and Class Members paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

130. Defendant failed to implement, or failed to effectively implement, the adequate data security practices, procedures, and programs to secure sensitive PII, as evidenced by the 2023 Data Breach.

131. As a result of Defendant's failure to implement the data security

practices, procedures, and programs required to adequately secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount of the funds paid by Plaintiffs and Class Members paid that Defendant reasonably and contractually should have expended on data security measures to secure their PII.

132. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII for which they paid.

133. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiffs' and the Class Members' PII, Plaintiffs and Class Members suffered, and continue to suffer, substantial injuries, including in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, actual harm and/or a continuing increased risk of harm.

Count IV
Breach of Implied Contract

134. Plaintiffs incorporates by reference the allegations in paragraphs 1 through 82 above as though fully set forth herein.

135. When Plaintiffs and Class Members provided their PII to Defendant in connection with seeking wireless voice, messaging, and data services, they entered into implied contracts in which Defendant agreed to comply with its statutory and

common law duties to protect Plaintiffs' and Class Members' PII.

136. Defendant required Plaintiffs and Class Members to provide PII to receive wireless voice, messaging, and/or data services.

137. Defendant affirmatively represented that it collected and stored the PII of Plaintiffs and Class Members using proper means.

138. Based on Defendant's representations and the requirements of Defendant for the use of its goods and services, Plaintiffs and Class Members accepted Defendant's offers and provided Defendant with their PII.

139. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised.

140. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

141. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII.

142. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: (i) representing that it would maintain adequate data privacy and security practices and procedures to safeguard the PII from unauthorized disclosures, releases, data breaches, and theft;

(ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections of Defendant's information systems; and (iii) failing to disclose to Plaintiffs and Class Members at the time they provided their PII that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

143. The 2023 Data Breach was a reasonably foreseeable consequence of Defendant's acts and omissions in breach of these contracts.

144. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to: (a) invasion of privacy; (b) actual identity theft; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2023 Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII in their continued possession; (g) future costs in terms of

time, effort, and money that will be expended as a result of the 2023 Data Breach for the remainder of the lives of Plaintiffs and other members of the proposed class; and (h) the diminished value of Plaintiffs' and Class Members' PII; (i) the diminished value of T-Mobile's services Plaintiffs and other members of the proposed class paid for and received; and/or (j) the actual and attempted sale of Plaintiffs' and Class Members' PII on the dark web.

Count V
Breach of Confidence

145. Plaintiffs incorporates by reference the allegations in paragraphs 1 through 82 above as though fully set forth herein.

146. At all relevant times, Defendant was fully aware of the confidential nature of Plaintiffs' and Class Members' PII.

147. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by promises and expectations that Plaintiffs and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, disclosed to, or viewed by unauthorized third parties.

148. Plaintiffs and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect the PII and not permit the PII to be accessed by, acquired by, disclosed to, or viewed by unauthorized third parties.

149. Plaintiffs and Class Members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect their PII, such as following basic principles of protecting their networks and data systems.

150. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' PII with the understanding that the PII would not be accessed by, acquired by, disclosed to, or viewed by the public or any unauthorized third parties.

151. Due to Defendant's failure to prevent, detect, and avoid the 2023 Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was accessed by, acquired by, disclosed to, or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

152. But for Defendant's failure to maintain and protect Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, disclosed to, or viewed by unauthorized third parties. Defendant's 2023 Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' PII, as well as the resulting damages.

153. As a direct and proximate result of Defendant's actions and omissions,

Plaintiffs and Class Members have suffered damages as alleged herein.

154. The injury and harm Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiffs' and Class Members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiffs' and Class Members' PII had security and other vulnerabilities that placed Plaintiffs' and Class Members' PII in jeopardy.

155. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2023 Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in T-Mobile's possession and is subject to further unauthorized disclosures so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as a result of the 2023 Data Breach for the remainder of the lives of

Plaintiffs and other Class Members; and (g) the diminished value of Plaintiffs' and Class Members' PII; (h) the diminished value of T-Mobile's services Plaintiffs and other members of the proposed class paid for and received; and/or (i) the actual and attempted sale of Plaintiffs' and Class Members' PII on the dark web.

Count VI
Breach of Contract

156. Plaintiffs incorporates by reference the allegations in paragraphs 1 through 82 above as though fully set forth herein.

157. Plaintiffs and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable contracts with Defendant.

158. Upon information and belief, these agreements include Defendant's affirmative obligations to keep its customers' sensitive PII private and secure.

159. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to benefit Plaintiffs and Class Members primarily and directly, as Defendant's business is not only to provide products and services for Plaintiffs and the Class, but also to safeguard the PII with which it was entrusted in connection with providing such products and services.

160. Upon information and belief, Defendant's representations required Defendants to implement the necessary security measures to protect Plaintiffs' and Class Members' PII.

161. Defendant materially breached its contractual obligations to protect Plaintiffs' and Class Members' PII when that information was accessed and exfiltrated as part of the 2023 Data Breach.

162. The 2023 Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of Plaintiffs' and Class Members' contracts.

163. As a direct and proximate result of the 2023 Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and loss of control of their PII, in addition to the present risk of suffering additional damages and out-of-pocket expenses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs is a proper representative of the Class requested herein;

B. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and

further relief as is just and proper;

C. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the public as requested herein, including, but not limited to:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Ordering Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

iv. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

v. Ordering Defendant to implement and maintain a comprehensive Information Security Program designed to protect the

confidentiality and integrity of the personal identifying information of Plaintiffs' and Class Members' personal identifying information;

vi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

vii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

viii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

ix. Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area

of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

x. Prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

xi. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

xii. Ordering that Defendant conduct regular database scanning and securing checks;

xiii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. Ordering Defendant to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Defendant's information network for both internal and external threats, and assess whether monitoring tools are appropriately configured, tested, and updated; and

xv. Ordering Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

D. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

E. An award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

F. An award of punitive damages; and

G. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and an award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury on all issues so triable.

DATED: January 31, 2023

HERMAN JONES LLP

By: */s/ John C. Herman*

John C. Herman
(Ga. Bar No. 348370)
Peter M. Jones
(Ga. Bar No. 402620)
Candace N. Smith
(Ga. Bar No. 654910)
Connely Doizé
(Ga. Bar No. 663453)

3424 Peachtree Road, N.E., Suite 1650
Atlanta, Georgia 30326
Telephone: (404) 504-6500
Facsimile: (404) 504-6501
jherman@hermanjones.com
pjones@hermanjones.com
csmith@hermanjones.com
cdoize@hermanjones.com

Counsel for Plaintiff